User guide of MISP Malware Information Sharing Platform, a Threat Sharing Platform.

MISP Contributors

Published with GitBook

Table of Contents

Introduction

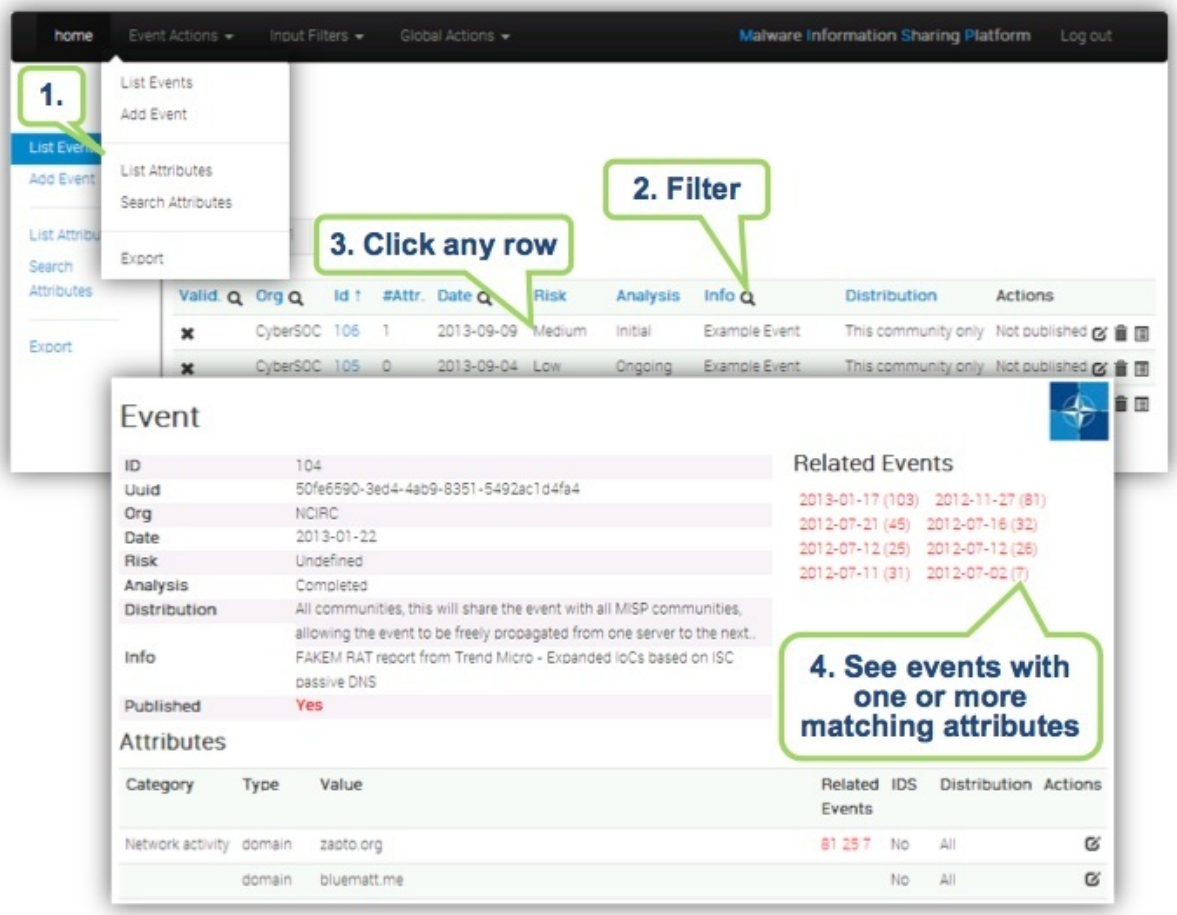
User guide of Malware Information Sharing Platform (MISP) - A Threat Sharing Platform

Quick Start

The Malware Information Sharing Platform (MISP) is the tool which will be used to facilitate the exchange of Indicator of Compromise (IOC) about targeted malware and attacks within your community of trusted members. It is a distributed Indicator of Compromise (IOC) database with technical and non-technical information. Exchanging this information should result in faster detection of targeted attacks and improve the detection ratio, while also reducing the number of false positives.

Create an Event

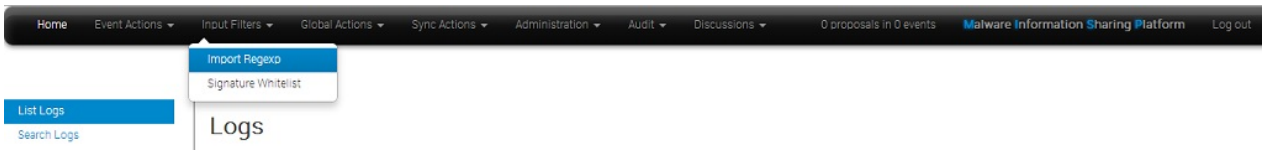
Browsing Events



Export Events for Log Search

General Layout

The top bar



This menu contains all of the main functions of the site as a series of dropdown menues. These contains all (from the current user's perspective) accessible functions sorted into several groups.

- **Home button:** This button will return you to the start screen of the application, which is the event index page (more about this later).
- **Event Actions:** All the malware data entered into MISP is made up of an event object that is described by its connected attributes. The Event actions menu gives access to all the functionality that has to do with the creation, modification, deletion, publishing, searching and listing of events and attributes.
- **Input Filters:** Input filters alter what and how data can be entered into this instance. Apart from the basic validation of attribute entry by type, it is possible for the site administrators to define regular expression replacements and blacklists for certain values in addition to blocking certain values from being exportable. Users can view these replacement and blacklist rules here whilst administrator can alter them.
- **Global Actions:** This menu gives you access to information about MISP and this instance. You can view and edit your own profile, view the manual, read the news or the terms of use again, see a list of the active organisations on this instance and a histogram of their contributions by attribute type.
- **Sync Actions:** With administrator access rights, shows a list of the connected instances and allows the initiation of a push and a pull (more about the synchronisation mechanisms later).
- **Administration:** Administrators can add, edit or remove user accounts and user roles. Roles define the access rights to certain features such as publishing of events, usage of the REST interface or synchronisation of any user belonging to the given role. Site administrators can also access a contact form, through which it is possible to reset the passwords of users, or to just get in touch with them via encrypted e-mails.
- **Audit:** If you have audit permissions, you can view the logs for your organisation (or for site admins for the entire system) here or even search the logs if you are interested in something specific.
- **Discussions:** Link to the discussion threads.
- **Proposal Notifications:** This shows how many proposals your organisation has received and across how many events they are spread out. Clicking this will take you to the list of proposals.
- **Log out:** Logs you out of the system.

A list of the contents of each of the above drop-down menues

Event actions

- **List Events:** Lists all the events in the system that are not private or belong to your organisation. You can add, modify, delete, publish or view individual events from this view.
- **Add Event:** Allows you to fill out an event creation form and create the event object, which you can start populating with attributes.
- **List Attributes:** Lists all the attributes in the system that are not private or belong to your organisation. You can modify, delete or view each individual attribute from this view.
- **Search Attributes:** You can set search terms for a filtered attribute index view here.
- **View Proposals:** Shows a list of all proposals that you are eligible to see.
- **Events with proposals:** Shows all of the events created by your organsiation that has pending proposals.

- **List Tags:**List all the tags that have been created by users with tag creation rights on this instance.
- **Add Tag:**Create a new tag.
- **List Templates:**List all of the templates created by users with template creation rights on this instance.
- **Add Template:**Create a new template.
- **Export:** Export the data accessible to you in various formats.
- **Automation:** If you have authentication key access, you can view how to use your key to use the REST interface for automation here.

Input filters

- **Import Regexp:** You can view the Regular Expression rules, which modify the data that can be entered into the system. This can and should be used to help filter out personal information from automatic imports (such as removing the username from windows file paths), having unified representation for certain common values for easier correlation or simply standardising certain input. It is also possible to block certain values from being inserted. As a site administrator or a user with regex permission, you can also edit these rules.
- **Signature Whitelist:** You can view the whitelist rules, which contain the values that are blocked from being used for exports and automation on this instance. Site administrators have access to editing this list.

Global Actions

- **News:** Read about the latest news regarding the MISP system
- **My Profile:** Manage your user account.
- **Members List:** View the number of users per organisation and get some statistics about the currently stored attributes.
- **Role Permissions:** You can view the role permissions here.
- **User Guide:** A link to this user guide.
- **Terms & Conditions:** View the terms & conditions again.
- **Statistics:** View a series of statistics about the users and the data on this instance.
- **Log out:** Logs the current user out.

Sync Actions

- **List Servers:** Connect your MISP instance to other instances, or view and modify the currently established connections.

Administration

- **New User:** Create an account for a new user for your organisation. Site administrators can create users for any organisation.
- **List Users:** View, modify or delete the currently registered users.
- **New Role:** Create a new role group for the users of this instance, controlling their privileges to create, modify, delete and to publish events and to access certain features such as the logs or automation.
- **List Roles:** List, modify or delete currently existing roles.
- **Contact Users:** You can use this view to send messages to your current or future users or send them a new temporary password.
- **Administrative Tools:** Various tools, upgrade scripts that can help a site-admin run the instance
- **Server Settings:** Set up and diagnose your MISP installation
- **Jobs:** View the background jobs and their progress
- **Scheduled Tasks:** Schedule the pre-defined tasks for your instance (this currently includes export caching, server pull and server push).

Audit

- **List Logs:** View the logs of the instance.
- **Search Logs:** Search the logs by various attributes.

Discussions

- **List Discussions:** List all of the discussion threads.
- **Start Discussion:** Create a new discussion thread.

The left bar

This bar changes based on each page-group. The blue selection shows you what page you are on.

General Concepts

Admins and Site Admins

There are two types of admins in MISP: Admins (also refered to as org admins) and Site Admins. Whilst the former can only do some limited administration of users of his/her own organisation, site admins have access to all of the features and data of the system. They are in charge of making sure that the system runs correctly and the maintenance of MISP.

Background Jobs

A lot of the heavier tasks are a burden to users, in that their actions can cause long delays (and in some cases timeouts) while the application logic is executing. To alleviate this, long processes have been (if enabled) moved to background jobs, meaning that their execution happens asynchronously in the background, allowing the user to freely interact with the platform whilst the request is being processed.

MISP Instance

A MISP instance is an installation of the MISP software and the connected database. All the data visible to the users is stored locally in the database and data that is shareable (based on the distribution settings) can be synchronised with other instances via the Sync actions. The instance that you are reading this manual on will be refered to as "this instance" or "your instance". The instances that your instance synchronises with will be refered to as "remote instances".

Organisation administrators and Site administrators

We have two types of administrators, site and organisation admins. The former has access to every administrator feature for all the data located on the system including global features such as the creation and modification of user roles and instance links, whilst organisation admins can administer users, events and logs of their own respective organisations.

Pivot path

The (branching) path taken by a user from event to event while following correlation links. This is represented by the branching graph in the event view.

Pivoting

The act of navigating from event to event through correlation links.

Proposals

Each event can only be directly edited by users of the original creator organisation (and site admins). However, if another organisation would like to amend an event with extra information on an event, or if they'd like to correct a mistake in an attribute, they can create a Proposal. These proposals could then be accepted by the original creator organisation. These proposals can be pulled to another server, allowing users on connected instances to propose changes which then could be accepted by the original creators on another instance (and subsequently pushed back).

Publishing

When an event is first created by a user, it is visible to everyone on the instance based on the access rights ("Your organisation only" events will not be visible to users of other organisations), but they will not be synchronised and they won't be exportable. For this, a user with publishing permission of the organisation that created the event has to publish the event. The system will then inform all the users of the instance that are subscribing to e-mail notifications and who have access to view the published event via an e-mail.

Pull

Pulling is the process of using the configured sync user on a remote instance to REST GET all of the accessible data (based on the distribution rights) to your instance and store it.

Push

Pushing is the process of using a configured instance link to send an event or all accessible events (limited by the distribution rights) through the REST interface to a remote instance.

Scheduled Tasks

Certain common tasks can be scheduled for a later execution or for regular recurring executions. These tasks currently include caching all of the export formats, pulling from all eligible instances and pushing to all eligible instances.

Sync User

A user of a role that grants sync permissions, these users (and their authentication keys) are used to serve as the points of connection between instances. Events pushed to an instance are pushed to a sync user, who then creates the events on the remote instance. Events pulled are added by the sync user that is used to connect the remote instance to your instance. As an administrator, keep in mind that a sync user needs auth key and publish permissions, has to have undergone the mandatory password change and has to have accepted the Terms of Use in order for the sync to work. Please make sure that all of these steps are taken before attempting to push or pull.

Synchronisation

What we call synchronisation is an exchange of data between two (or more) MISP instances through our pull and push mechanisms.

Tagging

Users with tagging rights can assigned various dynamically created tags to events, allowing an arbitrary link between events to be created. It is possible to filter events based on these tags and they can also be used to filter events for the automation.

Templating

Users with templating rights can create easy to fill forms that help with the event creation process.

Glossary

IOC

Indicator of compromise (IOC or IoC) is an artifact observed on a network or in an operating system or information channel that could reference an intrusion or a reference to a technique used by an attacker.

1. Quick Start

MISP

Malware Information Sharing Platform

0. Introduction 3. General Concepts 2. General Layout 1. Quick Start